# MATADRR

Mission Assurance, Threat Alert, Disaster Resiliency and Response

## Product Reference Guide

Revision 1.0

June 2014

# Report Documentation Page

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE | 2. REPORT TYPE | 3. DATES COVERED |
|---|---|---|
| **JUN 2014** | **N/A** | |

| 4. TITLE AND SUBTITLE | 5a. CONTRACT NUMBER |
|---|---|
| **Mission Assurance, threat Alert, Disaster Resiliency and Response (MATADRR) Product Reference Guide, June 2014** | 5b. GRANT NUMBER |
| | 5c. PROGRAM ELEMENT NUMBER |

| 6. AUTHOR(S) | 5d. PROJECT NUMBER |
|---|---|
| **Douglas Hardy /MATADRR, XM SPAWAR Systems Center Pacific (SSC Pacific) Christopher Russell, MATADRR DXM, SSC Pacific Contractor Support** | 5e. TASK NUMBER |
| | 5f. WORK UNIT NUMBER |

| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) | 8. PERFORMING ORGANIZATION REPORT NUMBER |
|---|---|
| **SPAWAR Systems Center, San Diego, CA 92152 (Code 53627)** | **SD 1228 June 2014 * JN14106** |

| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSOR/MONITOR'S ACRONYM(S) |
|---|---|
| **USNORTHCOM - MATADRR** | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) |

12. DISTRIBUTION/AVAILABILITY STATEMENT

**Approved for public release, distribution unlimited.**

13. SUPPLEMENTARY NOTES

**The original document contains color images.**

14. ABSTRACT

**Mission Assurance, Threat Alert Disaster Resiliency and Response (MATADRR) is USNORTHCOM's joint initiative to enhance automated information sharing and mission assurance by establishing information sharing interfaces across currently "stove piped" unclassified emergency management/force protection applications. Its goal is to quickly disseminate time-critical incidents, imminent threats, and/or hazard information within the USNORTHCOM Domestic Area of Responsibility to streamline information sharing through automation.**

15. SUBJECT TERMS

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | |
| **unclassified** | **unclassified** | **unclassified** | **UU** | **41** | |


*SD 1228*
*June 2014 • JN14106*
*Approved for public release.*

# Contents

## Figures

# 1 Introduction

The tragic shootings at Fort Hood in November 2009, at the Washington Navy Yard in September 2013, and again at Fort Hood in April 2014 have underscored the need to improve information sharing with partner agencies and among installations across the U.S. areas of responsibility. During the first two events (findings from the most recent Fort Hood incident are still being analyzed), installations in the surrounding area were not notified; U.S. Northern Command (USNORTHCOM) was not notified. Moreover, had either of these shootings been part of a coordinated attack, U.S. installations were unprepared to change their force protection posture. In response, USNORTHCOM developed a national information sharing middleware to change this dynamic. Across the country, organizations are able to overcome technical challenges and institutionalize information sharing across disparate government and commercial emergency management and force protection systems.

## The MATADRR Mission

Mission Assurance, Threat Alert, Disaster Resiliency and Response (MATADRR) is USNORTHCOM's joint initiative to enhance automated information sharing and mission assurance by establishing information sharing interfaces across currently "stove-piped" unclassified emergency management/force protection (EM/FP) applications. Its goal is to quickly disseminate time-critical incidents, imminent threats, and/or hazard information within the USNORTHCOM Domestic Area of Responsibility (AOR) to streamline information sharing through automation.

## The Keystone Solution

In response to the requirement to more efficiently share information without negatively impacting current system investments and EM/FP operations, the MATADRR initiative developed a middleware software capability named Keystone. Keystone is based on the Unified Incident Command and Decision Support (UICDS) software.

Keystone is a standards-based middleware that receives, translates, and transmits incident related data between linked disparate systems to allow a common view between them. As middleware, Keystone does not interface directly with end users. Keystone is the transporter of uniform data in common formats. Emergency applications (sensors, incident logs, personnel management, dispatch systems, video surveillance and intelligence tools – anything related to homeland security) can provide a portion of their data to Keystone, which then publishes it to subscribers' applications. The applications then see the consumed data inside their own user interface. Thus, to the user, there is no new application, no new learning, and no conscious sending of information. Further, Keystone is not intended to replace current standard operating procedures, messages and/or reports for communicating emergency management and force protection data. It is intended to enhance, enable and more quickly disseminate emergency management and force protection data to a broader community of recipients. Paramount to Keystone success is the concept of improved local and regional awareness, with simultaneous national awareness, available to decision makers at all levels in between.

By using data standards, by managing data content, by ensuring two-way sharing of data, by protecting data ownership, and by defining the minimal fraction of data needed for collaborative decision making, Keystone is allowing organizations to work within their own existing concepts of operations using their own prior technology investments to achieve information sharing.

## Purpose

This document describes the MATADRR Keystone products and related non-materiel solutions. It identifies the organizations (with key points of contact [POCs]) using the Keystone solution, how each customized the solution, and how they agreed to transition it. Most importantly, this document provides information for obtaining Keystone products and support. Lastly, the document contains artifact information for use in Defense Technical Information Center (DTIC) for future programs and projects.

# 2 Transition Products

The goal of MATADRR is to share information across domains, roles, functions, hazards, and applications – not to create a new application that everyone must use. The MATADRR project uses the Keystone software to provide true information sharing among applications that enable each individual application – selected for its intrinsic value by an end-user organization – to acquire common data and compose that data into a visualization that is appropriate for the end user (Figure 1). The application then can further process that data and resubmit it for sharing with the originating – and other interested – applications. Keystone is not one size fits all; one application cannot meet all needs. Keystone builds many-to-many relationships among applications to meet the unique needs of very diverse end-user communities created by the Concept of Operations (CONOPS) the communities construct.

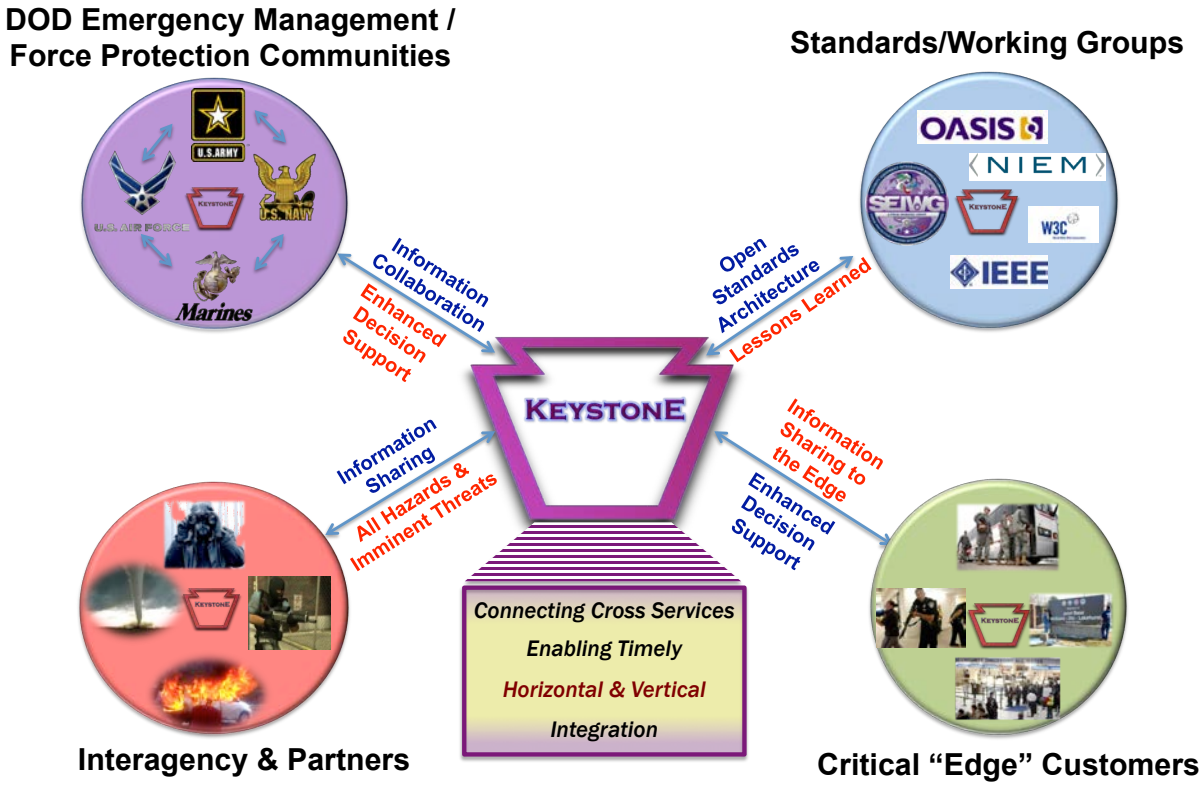



*Figure 1. MATADRR Operational View*

## Keystone Architecture Overview

The Keystone architecture is constructed of two main web services: the Core and the software adapters (Figure 2). The Core manages infrastructure and services while the software adapters perform the actual translations. The architecture is built on service-oriented principles using open standards. Each Keystone Core serves as a local point of integration. Keystone Cores support three varieties of services: infrastructure, domain, and external. Infrastructure services enable the sharing of information between Cores and are based on existing, established industry standards. Domain services provide for the sharing of translated information specific to EM/FP, such as all hazards and threats, incidents, command hierarchies, tasking, and shared awareness. These services rely on existing and developing standards in the EM/FP domains – such as those from National Information Exchange Model (NIEM) and the Organization for the Advancement of Structured Information Standards (OASIS) EM Technical Committees. In addition, each Core provides the ability to register external services using existing, developing and future standards.

### *Scalability*

A valuable feature of the Keystone architecture is its scalability. That is, Keystone can be modified to serve any type or size of community. The Keystone Core can be deployed as a simple stand-alone system for a few sites or as a system of distributed networked Cores.

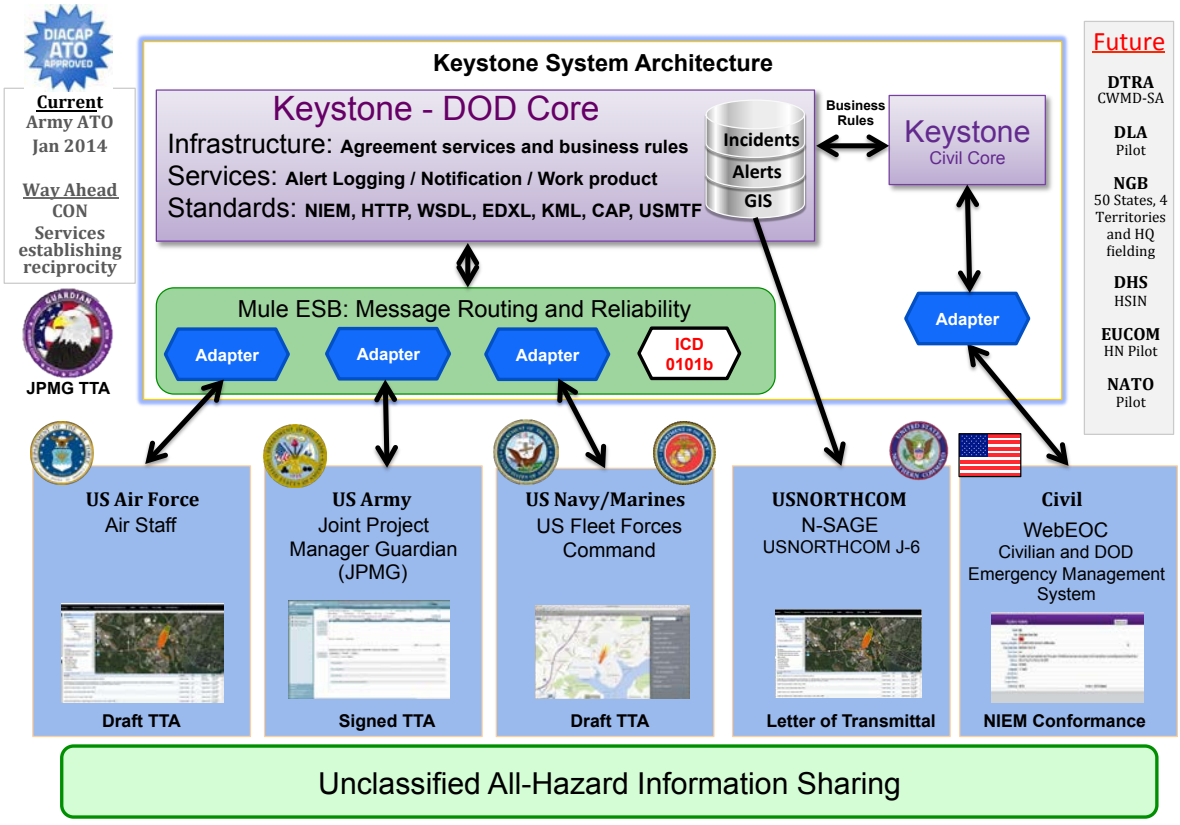



*Figure 2. Keystone Architecture*

## Contact Information

### *Program Manager*

USNORTHCOM
Jorge Zambrana
jorge.zambrana@northcom.mil
719-556-7457

### *Transition Manager*

SPAWARSYSCENPAC
Doug Hardy
douglas.hardy@navy.mil
619-553-5410

### *Technical Manager/ Performer*

ARDEC

Robert Giarratano
robert.m.giarratano.civ@mail.mil
973-724-8096

Italo Grasso
italo.g.grasso.civ@mail.mil
973-724-8052

# Keystone Core

***Technology Readiness Level:*** *6+*

***Deliverables:*** *Source code, software executable files, business rules, documentation and information assurance data*

### *Description*

As stated previously, the Keystone Core manages domain services and infrastructure services. Domain services include incident management, incident commands, incident action plans, tasking, alerts, maps, resources, and sensors. Infrastructure services include agreements, profiles, notifications, work products, directories, and broadcasts.

The Cores are configured to support agreements, for the exchange of data. Agreements follow local Memorandums of Understanding (MOUs) and/or Mutual Aid Agreements (MAAs) that define the terms and conditions under which service component installations will share information. Agreements must be mutually established prior to data sharing and enable dynamic, all hazards and threats data sharing topologies.

### *Deployment*

Keystone Cores can be installed on any virtual machine and network depending on the governance and policies of the participating organizations. Cores can be hosted by a government agency for several other agencies, or by a state for many of its local jurisdictions. Core hosting can be outsourced for those sites that do not have the requisite information technology infrastructure.

# Keystone Adapters and Interfaces

### *Description*

Keystone adapters perform the following functions:

- Integrate other national message sharing programs (e.g., Integrated Public Alert and Warning System [IPAWS], Federal Emergency Management Agency [FEMA]; Common Alerting Protocol [CAP], Oasis)
- Integrate commercial and government data aggregator applications (e.g., AtHoc©, Installation Protection Integration Platform [iP2], Command, Control, Communication, Computers, and Intelligence Suite [C4IS], Non-Secure Internet Protocol Router Situational Awareness Geospatial Enterprise [NIPR-SAGE], WebEOC®, Interface Control Document [ICD]-0101B)
- Provide two-way information sharing among commercial and government incident management technologies to achieve collaborative decision making

- Correlate information from all these sources into defined incidents, meaning that all relevant information about an incident can be available from one source – Keystone
- Provide content management for information associated with incidents so that connected applications know that they are getting the latest, authoritative source data available

### *How It Works*

When an organization installs Keystone, it sets up secure sharing exchange agreements that define how and with whom it will share its information. Data owners continue to compose their data as usual within their own specific system/domain. Keystone then builds a defined incident about an event by compiling a series of Keystone Work Products composed of data provided by applications interfaced to Keystone through the application's Keystone Adapter. The adapter authenticates the application to connect to Keystone Web Services and translates the detailed data of the application into the fractional data in a standard format to be shared through Keystone. Thus, the Keystone Work Product is the basic unit of data exchange among applications. Each application provides data when it has something to contribute to the incident knowledge base and consumes a work product when it wants its end user to know about the incident.

All adapters can reside on an Enterprise Service Bus (ESB), which provides support for messaging reliability, security, performance, and translation to and from standard formats, such as, CAP, National Incident Management System (NIMS) and NIEM. New adapters can easily be added using the Software Development Kit (SDK).

### *Currently Available Interfaces and Adapters*

A number of adapters and interfaces have already been developed*. These adapters/interfaces and the communities they represented for the MATADRR project are listed as follows:

- iP2 (Army)
- C4IS (Navy)
- AtHoc (Air Force)
- NIPR-SAGE (USNORTHCOM)
- WebEOC (Civilian)
- ICD-0101B (prototype)

*Development of adapters to commercial products does not define an endorsement by the Government for these systems.

## Contact Information

### *Program Manager*

USNORTHCOM
Jorge Zambrana
jorge.zambrana@northcom.mil
719-556-7457

### *Transition Manager*

SPAWARSYSCENPAC
Doug Hardy
douglas.hardy@navy.mil
619-553-5410

### *Technical Manager/ Performer*

ARDEC

Robert Giarratano
robert.m.giarratano.civ@mail.mil
973-724-8096

Italo Grasso
italo.g.grasso.civ@mail.mil
973-724-8052

# iP2 Adapter

***Technology Readiness Level:*** *6+*

***Deliverables:*** *Source code, software executable files, Army suggested business rules, documentation and information assurance data*

## *Description*

Installation Protection Integration Platform (iP2) is an emergency response and information management system focused on the incident command post (ICP) to emergency operations center interface with “All Hazards” capable functionality. iP2 provides an integration platform that facilitates interoperability and provides a common operating picture (COP) that enables situational awareness for onscene response and offscene support personnel during all phases of incident management activities. The primary operators of the system are Department of Defense (DoD) civilians to include installation emergency management personnel, decision makers and first responders.

## *Client Type*

Current R14.01 (iP2 V7.1.2)
ip2->Keystone http connection, REST interface
Keystone->ip2 http connection, REST interface
R14.06 proposed (iP2 V7.2.0)
iP2->Keystone jms connection, tcp over SSL, JAXB interface, pub/sub topics - client to broker
Keystone->iP2 jms connection, tcp over SSL, JAXB interface, pub/sub topics - broker to client

## *Data Format*

R14.01
iP2 XML (see iP2 API documents for object model)
R14.06 proposed
JAXB messaging objects (see iP2 JAXB data model)

## *Communication Flow*

- Create/Update incidents
- Incident sharing
- Plume sharing
- Bidirectional
  - iP2 to Keystone Core
  - Keystone Core to iP2

## Contact Information

### *Program Manager*

USNORTHCOM
Jorge Zambrana
jorge.zambrana@northcom.mil
719-556-7457

### *Transition Manager*

SPAWARSYSCENPAC
Doug Hardy
douglas.hardy@navy.mil
619-553-5410

### *Technical Manager/ Performer*

ARDEC

Robert Giarratano
robert.m.giarratano.civ@mail.mil
973-724-8096

Italo Grasso
italo.g.grasso.civ@mail.mil
973-724-8052

# C4IS Adapter


***Technology Readiness Level:*** *6+*

***Deliverables:*** *Source code, software executable files, Navy suggested business rules, documentation and information assurance data*

## *Description*

Command, Control, Communication, Computers, and Intelligence Suite (C4IS) is a SharePoint® and web-based application that assists the Navy shore command in response to the "All Hazard Approaches" to threats, providing a multi-tiered approach to developing Situational Awareness (SA) in support of the security, safety and the integrity of Navy installations and forces.

The C4IS adapter consists of a mediation adapter and a Mule-ESB adapter. The C4IS adapter implements the "Notice Type" type-"ATFP" of Urgent Notice messages. The mediation server is responsible for the communication between C4IS system and the Mule-ESB adapter. The Mule-ESB adapter is responsible for the communication between the mediation adapter and the Keystone Core. The mediation server is transitional into the Keystone accreditation boundary and will eventually be merged as part of the Mule-ESB adapter in the future.

## *Client Type*

HTTPS (Hypertext Transfer Protocol Secure)

## *Data Format*

Urgent Notice XML data format sent/receive between C4IS/Keystone

## *Communication Flow*

- Create/Update incidents
- Incident sharing
- Alert sharing
- Plume sharing
- Bidirectional
  - C4IS to Keystone Core
  - Keystone Core to C4IS

## Contact Information

### *Program Manager*

USNORTHCOM
Jorge Zambrana
jorge.zambrana@northcom.mil
719-556-7457

### *Transition Manager*

SPAWARSYSCENPAC
Doug Hardy
douglas.hardy@navy.mil
619-553-5410

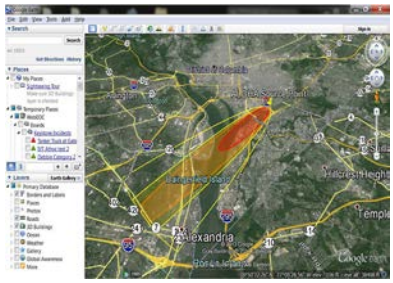
### *Technical Manager/ Performer*

ARDEC

Robert Giarratano
robert.m.giarratano.civ@mail.mil
973-724-8096

Italo Grasso
italo.g.grasso.civ@mail.mil
973-724-8052

# WebEOC Adapter



***Technology Readiness Level:*** *6+*

***Deliverables:*** *Source code, software executable files, Civilian suggested business rules, documentation and information assurance data*

## *Description*

Web Based Emergency Operations Center (WebEOC®) is a web-enabled and locally-configurable incident and event management system. With access to the Internet, authorized emergency managers and first responders, regardless of location, can enter and view incident information in WebEOC status boards. WebEOC enables users to manage multiple incidents and daily events, assign and track missions and tasks, provide situation reports, manage resources, and prepare Incident Command System (ICS) and Incident Action Plan (IAP) reports. WebEOC is used by federal, state, county and city entities.

## *Client Type*

HTTP Polling

## *Data Format*

WebEOC XML

## *Communication Flow*

- Create/Update incidents
- Incident sharing
- Plume sharing
- Bidirectional
  - WebEOC to Keystone Core
  - Keystone Core to WebEOC

## Contact Information

### *Program Manager*

USNORTHCOM
Jorge Zambrana
jorge.zambrana@northcom.mil
719-556-7457

### *Transition Manager*

SPAWARSYSCENPAC
Doug Hardy
douglas.hardy@navy.mil
619-553-5410

### *Technical Manager/ Performer*

ARDEC

Robert Giarratano
robert.m.giarratano.civ@mail.mil
973-724-8096

Italo Grasso
italo.g.grasso.civ@mail.mil
973-724-8052

# AtHoc Adapter


***Technology Readiness Level:*** *6+*

***Deliverables:*** *Source code, software executable files, Air Force suggested business rules, documentation and information assurance data*

## *Description*

AtHoc IWSAlerts™ provides enterprise-class, network-centric mass notification and emergency communication systems customized for military, government, healthcare, higher education and commercial organizations. The AtHoc solutions automate the end-to-end emergency communication process, delivering physical security, force protection, situational awareness, and personnel accountability. Allow communication between AtHoc and other Emergency Management Systems via Keystone.

## *Client Type*

AtHoc -> Keystone: HTTP Post to AtHoc SDK (polling)
Keystone -> AtHoc: HTTP Post to AtHoc SDK

## *Data Format*

AtHoc XML: see AtHoc SDK Manual

## *Communication Flow*

- Create/Update incidents
- Incident sharing
- Plume sharing
- Bidirectional
  - AtHoc to Keystone Core
  - Keystone Core to AtHoc

## Contact Information

### *Program Manager*

USNORTHCOM
Jorge Zambrana
jorge.zambrana@northcom.mil
719-556-7457

### *Transition Manager*

SPAWARSYSCENPAC
Doug Hardy
douglas.hardy@navy.mil
619-553-5410

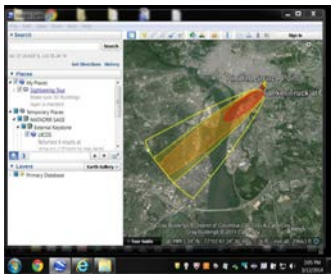
### *Technical Manager/ Performer*

ARDEC

Robert Giarratano
robert.m.giarratano.civ@mail.mil
973-724-8096

Italo Grasso
italo.g.grasso.civ@mail.mil
973-724-8052

# NIPR-SAGE Interface



***Technology Readiness Level:*** *6+*

***Deliverables:*** *Source code, software executable files, USNORTHCOM suggested business rules, documentation and information assurance data*

## *Description*

U.S. Northern Command's Situational Awareness Geospatial Enterprise (SAGE) bridges the gap between disparate situational awareness systems by integrating critical infrastructure, force tracking, interagency, and incident management data at the unclassified, NIPRnet level. USNORTHCOM has taken a full service oriented architecture (SOA) approach to providing data both at USNORTHCOM headquarters and throughout the unclassified DoD community in support of Homeland Defense and Homeland Security efforts.

SAGE is a robust Geographic Information Systems (GIS) architecture designed to distribute and empower all USNORTHCOM Mission Partners with actionable geospatial data anywhere in the world. Keystone implants the Google Earth KML (Keyhole Markup Language) publishing interface to consume the Keystone Work Product sharing.

## *Client Type*

Google Earth KML interface

## *Data Format*

Consume Keystone Work Product XML data format

## *Communication Flow*

Unidirectional: Keystone Core to NIPR-SAGE

## Contact Information

### *Program Manager*

USNORTHCOM
Jorge Zambrana
jorge.zambrana@northcom.mil
719-556-7457

### *Transition Manager*

SPAWARSYSCENPAC
Doug Hardy
douglas.hardy@navy.mil
619-553-5410

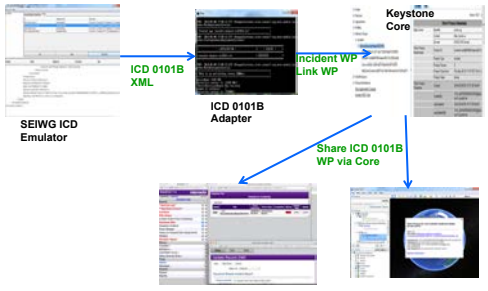
### *Technical Manager/ Performer*

ARDEC

Robert Giarratano
robert.m.giarratano.civ@mail.mil
973-724-8096

Italo Grasso
italo.g.grasso.civ@mail.mil
973-724-8052

# ICD 0101B Adapter (Prototype)




***Technology Readiness Level:*** *4+*

***Deliverables:*** *Source code, software executable files, documentation*

## *Description*

The Interface Control Document (ICD) - 0101B (ICD-0101B) adapter prototype employs the Army's Security Equipment Integration Working Group (SEIWG) Extensible Markup Language (XML) communication standard to interface with multiple types of sensors messages via the SEIWG sensor emulator. The ICD-0101B adapter provides message translation services by transforming SEIWG formatted ICD-0101B device status and device incident XML messages into Keystone work products such as the incident and the link work products on the Keystone core. These work products are then shared via the core to other adapters such as NIPR SAGE and AtHoc.

## *Client Type*

R14.01
SEIWG Emulator -> ICD-0101B adapter -> HTTP Post to Keystone SOAP web service -> External Clients (NIPR-SAGE Google Earth, AtHoc)

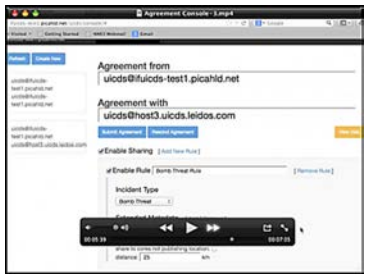
## *Data Format*

SEIWG XML Messages – (See SEIWG ICD)

## *Communication Flow*

- ICD-0101B adapter polls SEIWG emulator for sensor events
- SEIWG emulator sends sensor events
- ICD-0101B adapter translates sensor event into SOAP request
- Create work products on Keystone core

# Keystone Administrative Console / Agreement Services




***Technology Readiness Level:*** *4+*

***Deliverables:*** *Source code, software executable files, business rules, and documentation*

## Contact Information

### *Program Manager*

USNORTHCOM
Jorge Zambrana
jorge.zambrana@northcom.mil
719-556-7457

### *Transition Manager*

SPAWARSYSCENPAC
Doug Hardy
douglas.hardy@navy.mil
619-553-5410

### *Technical Manager/ Performer*

ARDEC

Robert Giarratano
robert.m.giarratano.civ@mail.mil
973-724-8096

Italo Grasso
italo.g.grasso.civ@mail.mil
973-724-8052

### *Description*

The **Administrative Console** is the graphical user interface to the Keystone Core for system administrators. It provides the means to establish and define relationships between Keystone Cores and Keystone Adapters through their associated incident management applications. An administrator can create resource profiles to allow subscription to the data in the Core; set up sharing agreements between multiple Cores; display, close and archive incidents and work products; and monitor the health and status of the Core.

**Agreement Services** are enabled through the Administrative Console. Agreement Services include sharing data by incident/event type, specified incident, proximity (range), and specific metadata. The Agreement Services are normally predefined and allow information sharing relationships based on Mutual Aid Agreements, Memorandums of Agreements, Memorandums of Understanding, and other contractual documents between organizations.

## Contact Information

### *Program Manager*

USNORTHCOM
Jorge Zambrana
jorge.zambrana@northcom.mil
719-556-7457

### *Transition Manager*

SPAWARSYSCENPAC
Doug Hardy
douglas.hardy@navy.mil
619-553-5410

### *Technical Manager/ Performer*

ARDEC

Robert Giarratano
robert.m.giarratano.civ@mail.mil
973-724-8096

Italo Grasso
italo.g.grasso.civ@mail.mil
973-724-8052

# Keystone Software Development Kit (SDK)

### *Description*

The Keystone Software Development Kit (SDK) provides developers with tools to develop, build and test their application adapters with the Keystone core. The SDK package provides code examples, as well as, supporting documentation, as described below.

### *SDK Documentation*

All documentation is currently in-progress and stamped DRAFT. All documentation is releasable to the DoD and U.S. DoD contractors only. The following is the current list of DRAFT SDK documents available:

- Architecture Description Document (ADD)
- Interface Design Description (IDD) - CORE Only
- System-Subsystem Design Document (SDD)
- Universal CONOPS
- Quick Start Reference Guide
- Installation Guide

Other transition documents will include the following documents:

- Build Procedures
- Software Version Description
- Business Rules Manual
- Software Release Notes

### *SDK Request*

An initial release (beta) of the MATADRR Keystone Software Development Kit (SDK) is available upon request. To request a copy of the current SDK release, please send an e-mail to Mike Cazzola (michael.w.cazzola@civ.mail.mil). The e-mail must include the following:

- Your Name
- Your E-Mail
- Your Phone
- Your Organization and Location
- Your Project Name and Government Sponsor
- Technical POC Name (person who will be receiving SDK)
- Technical POC E-Mail
- Technical POC Phone

You will be contacted with information on the process for receiving the documents and support.

## Keystone Authorization to Operate (ATO)

The authority to operate for Keystone was approved effective 16 January 2014 with an Authorized Termination Date of 15 January 2017. This application is approved as a Type ATO at the MAC II/Sensitive level.

The next step for the Authorization to Operate is to generate the individual packages for the Navy and Air Force based on the approved Army ATO Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) package. The intent is to have Keystone deployable on all NIPR networks.

A Certificate of Networthiness request was submitted on 19 February 2014. Keystone passed its Network Enterprise Technology Command (NETCOM) analyst review and is awaiting signature by the NETCOM approving official.

Along with the Certificate of Networthiness and the Authority To Operate (ATO), the executive DIACAP package will be provided including the following Information Assurance documents:

- Certificate of Networthiness (CoN)
- Authority To Operate (ATO)
- System Identification Profile (SIP)
- DIACAP Scorecard
- Information Technology (IT) Security Plan of Action & Milestones (POA&M)

### Contact Information

***Program Manager***

USNORTHCOM
Jorge Zambrana
jorge.zambrana@northcom.mil
719-556-7457

***Transition Manager***

SPAWARSYSCENPAC
Doug Hardy
douglas.hardy@navy.mil
619-553-5410

***Technical Manager/ Performer***

ARDEC

Robert Giarratano
robert.m.giarratano.civ@mail.mil
973-724-8096

Italo Grasso
italo.g.grasso.civ@mail.mil
973-724-8052

# 3 Transition Partners and Agreements

## Technology Transition Agreements

The MATADRR Technology Transition Agreements (TTAs) are collaborative documents between the Product Agent, USNORTHCOM MATADRR Operational Manager, and key Sustaining Agents (e.g., typically programs of record providing long-term maintenance of the product and/or components). The key terms of the agreements include:

- A list of the specific products to be delivered by the Product Agent.
- Any known critical gaps or capability shortfalls, and their fixes (within budget and schedule constraints) before the product delivery will be accepted by the Sustaining Agent.
- Any acceptance events defined by the Product Agent and Sustaining Agent (e.g., Technical Demonstrations, Independent Verification and Validation [IV&V] events, Operational Utility Assessments).
- A projected timeline for the final acceptance and transition of the product to the Sustaining Agent.

## Transition Partners

A MATADRR TTA was signed between USNORTHCOM and JPM Guardian on 12 July 2013 to transition the Keystone product. Other TTAs were drafted and a final draft has been staffed with the US Fleet Forces Command pending further definition and refinement of the Concept of Employment documentation.

More recently a letter has been staffed from USNORTHCOM to the JPEO-CBD to endorse JPM Guardian as the Joint Product Office. Therefore, it is now the intent of MATADRR Management to provide Letters of Transmittal to provide the Keystone product to the existing Transition Partners as noted in the table below.

***Figure 3. JPMG TTA Signatories***

| ORGANIZATION | TRANSITION PARTNER | TRANSITION OWNER | TRANSITION AGREEMENT |
|---|---|---|---|
| U.S. Army | Joint Project Manager Guardian (JPMG) | Ms. Karen House | Technology Transition Agreement (TTA) |
| U.S. Navy | Fleet Forces Command (NAVNORTH) | CDR Paul Bunnell | Draft TTA, Transmittal Letter |
| National Guard Bureau | Command, Control, Communications, and Computers Directorate (J-6) | LTC Tim Pettit | Transmittal Letter |
| U.S. Air Force | Headquarters Air Force (A-4/7) | Lt Col William Lowery | Transmittal Letter |

### *Deliverables*

| KEYSTONE PRODUCT DELIVERABLE PACKAGE |
|---|
| **Software** |
| ■ Keystone Source Code* |
| ■ Executables |
| **Documentation** |
| *SDK Documents* |
| ■ Architecture Description Document (ADD) |
| ■ Interface Design Document (IDD) – Core Only |
| ■ System Subsystem Design Document (SDD) |
| ■ Quick Start Reference Guide |
| ■ Installation Guide |
| ■ Universal CONOPS |
| *Information Assurance Documents* |
| ■ Army DIACAP Package |
| ■ Army CoN Package |
| ■ Army ATO (Authority to Operate) |
| *Other Documents* |
| ■ Software Version Description |
| ■ Build Procedures |
| ■ Software Release Notes |
| ■ Test Procedures, Scripts, Scenarios, Data |
| ■ Business Rules User's Manual |
| **Training/Product Support** |
| ■ Training Materials (Briefing Slides, Usage Scenarios) |
| ■ Product Support (Help Desk process and information) |

*In accordance with the ATO, ARDEC is responsible for the integrity of the software code. Therefore, the Keystone software code shall remain under ARDEC's Configuration Management Control.

# 4 Transition Acceptance Events

This section outlines Keystone's move from the science and technology (S&T) development stage to a product ready to be used in an operational environment: ready to prevent/respond to an incident or to alert/receive alerts from other partners. Acceptance events were increasingly operationally focused demonstrations and/or exercises intended to improve the transition readiness of the software to the receiving program. In the end, successful test and assessment reports led to a product acceptance letter between the TTA organizations, indicating the receiving program's intention of integrating the Keystone product into its software baseline.

## Technology Demonstration (Ft. Belvoir)

The MATADRR Technology Demonstration took place on 25 June 2013 in Fort Belvoir, VA. The demonstration went as planned; the Keystone Cores, adapters and five emergency management applications operated as expected.

### *Demonstration Scenario*

The demonstration scenario was based on an incident at Fort Belvoir, VA, in which a tank truck, carrying fuel, explodes near the Pence Gate (the main entrance to Fort Belvoir). The flames from the truck spread, creating a large fire and plume cloud at the gate that spread to the surrounding area including U.S. Route 1.

- The Army IP2 system transmitted an Incident Message with a plume model. This information was then shared across services with the local Navy and Air Force respective emergency management systems.
- The Air Force system for this demonstration, AtHoc, transmitted a notification text message (which was converted to speech) to select telephone (cellular and landline) as a personnel notification method for the Air Force.
- The Navy C4IS system transmitted a notification as an urgent message to the affected Navy areas.
- At a higher echelon, USNORTHCOM's situational awareness NIPR-SAGE system received the incident information by receiving a URL link to the incident and plume model information, where it was added to the NIPR-Sage MATADRR menu. Users with the proper access ID were able to access the NIPR-Sage plume model link via Google Earth.
- And because of potential impact to the local county, the information was shared to WebEOC representing Fairfax County's EM system (local civilian first responders).

Figure 4 depicts the information flow of data within the MATADRR construct for this demonstration.

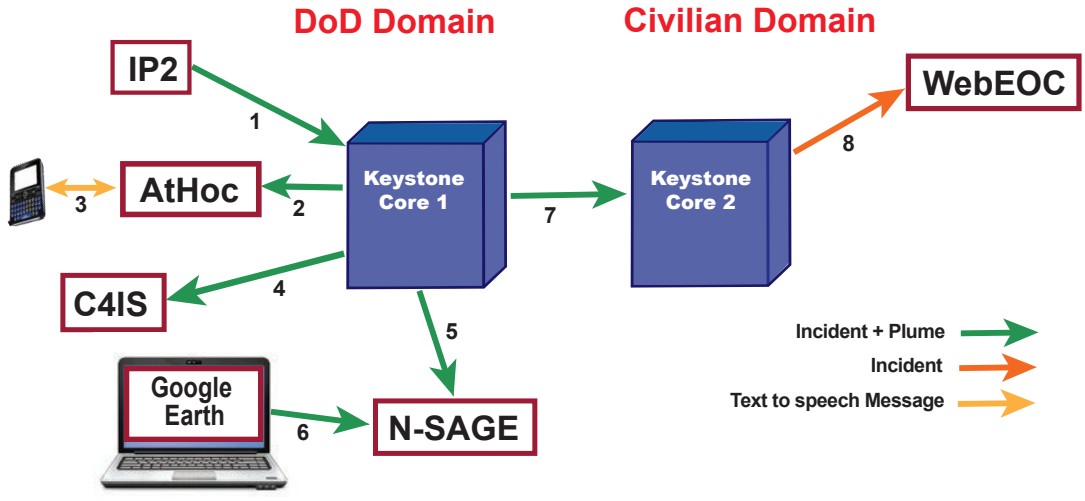



*Figure 4. Technology Demonstration Data Flow*

There were approximately 50 people in attendance for the demonstration. The feedback regarding the concept and application was positive: “MATADRR is already where we need other systems to be in the purple (Joint)” – Colonel Dennis. Constructive feedback was mostly related to the complexity of the demonstration and suggestions for improvement.

The MATADRR web site (http://www.matadrr.org) contains a video (Figure 5) from that demonstration showing:

- How MATADRR shares information across services (iP2, C4IS, AtHoc, WebEOC, and NIPR-SAGE)
- Scalability of information, by transferring information across multiple Keystone Cores
- Examples of MATADRR business rules which are the tools of content management

*Figure 5. MATADRR Demonstration Video*

## Independent Verification Test (San Diego)

The MATADRR Independent Verification Test (IVT) took place from 18 February to 14 March 2014 in San Diego, CA. It consisted of the MATADRR-developed Keystone Cores and Keystone Adapters, along with third-party applications (Figure 6). Additions to the IVT, that went beyond the original Technical Demonstration at Ft. Belvoir, included updates to AtHoc and WebEOC applications, and an ICD-0101B prototype.

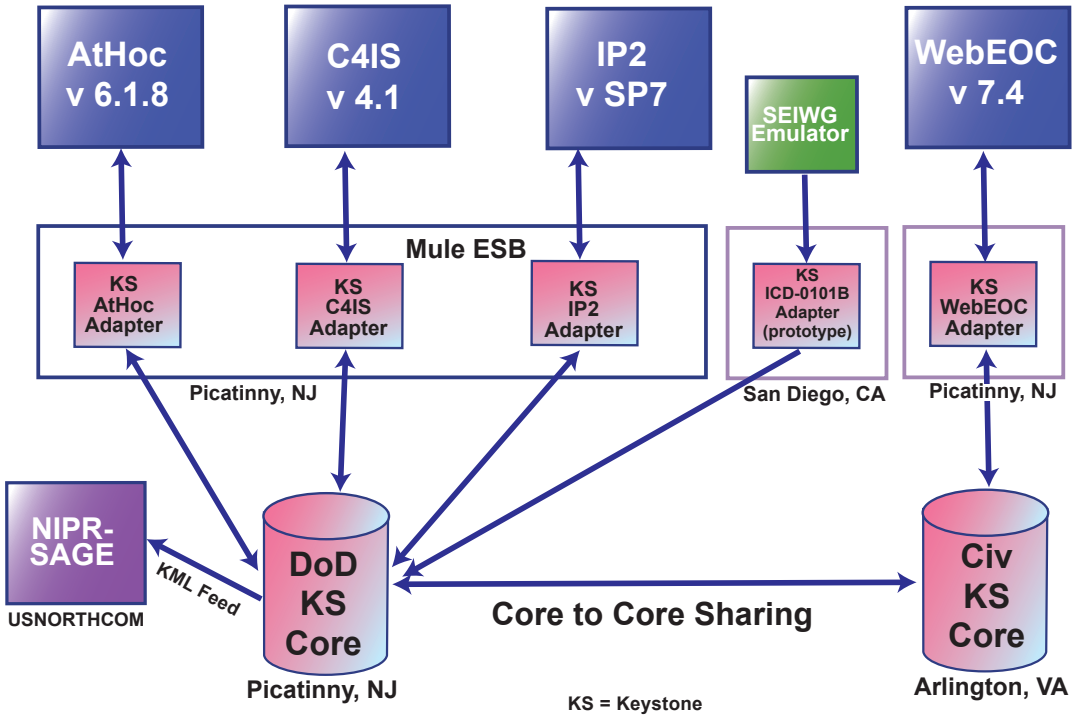



*Figure 6. MATADRR IVT Test Architecture*

For this test and demonstration event, one Keystone Core and all of the Keystone Adapters were deployed at Armaments Research Development and Engineering Center (ARDEC), Picatinny Arsenal, NJ. This demonstrated the hub-spoke, client-server type of architecture. Another Keystone Core was deployed at a contractor facility in Arlington, VA. Multiple Cores were used to demonstrate the scalability and peer-to-peer type of architecture.

All third-party applications were deployed at different locations across the country as indicated by blue dots on the associated map (Figure 7). These applications included iP2, C4IS, AtHoc, WebEOC, and NIPR-SAGE. All communications across the applications were done through the Keystone Adapters, which utilized Keystone Cores to share information. All communications were bi-directional, with the exception of the NIPR-SAGE application that only received data (KML).

All IVT Testers and Operators were operating from San Diego and utilized the web clients of each application to send and receive information. The Testers and Operators, while located in San Diego for this event, could have been geographically dispersed.

The IVT concluded on 14 March 2014. Initial findings indicated that 98% of test cases were successful, with no immediate or urgent problem change requests. Business rules were tested, end-to-end scenario tests were executed in preparation for the Final Transition Demonstration (FXD), and the Joint Interoperability Test Command (JITC) successfully collected their data for interoperability assessment. The official results from the IVT will be available in early May, and the JITC assessment is scheduled for mid-May.

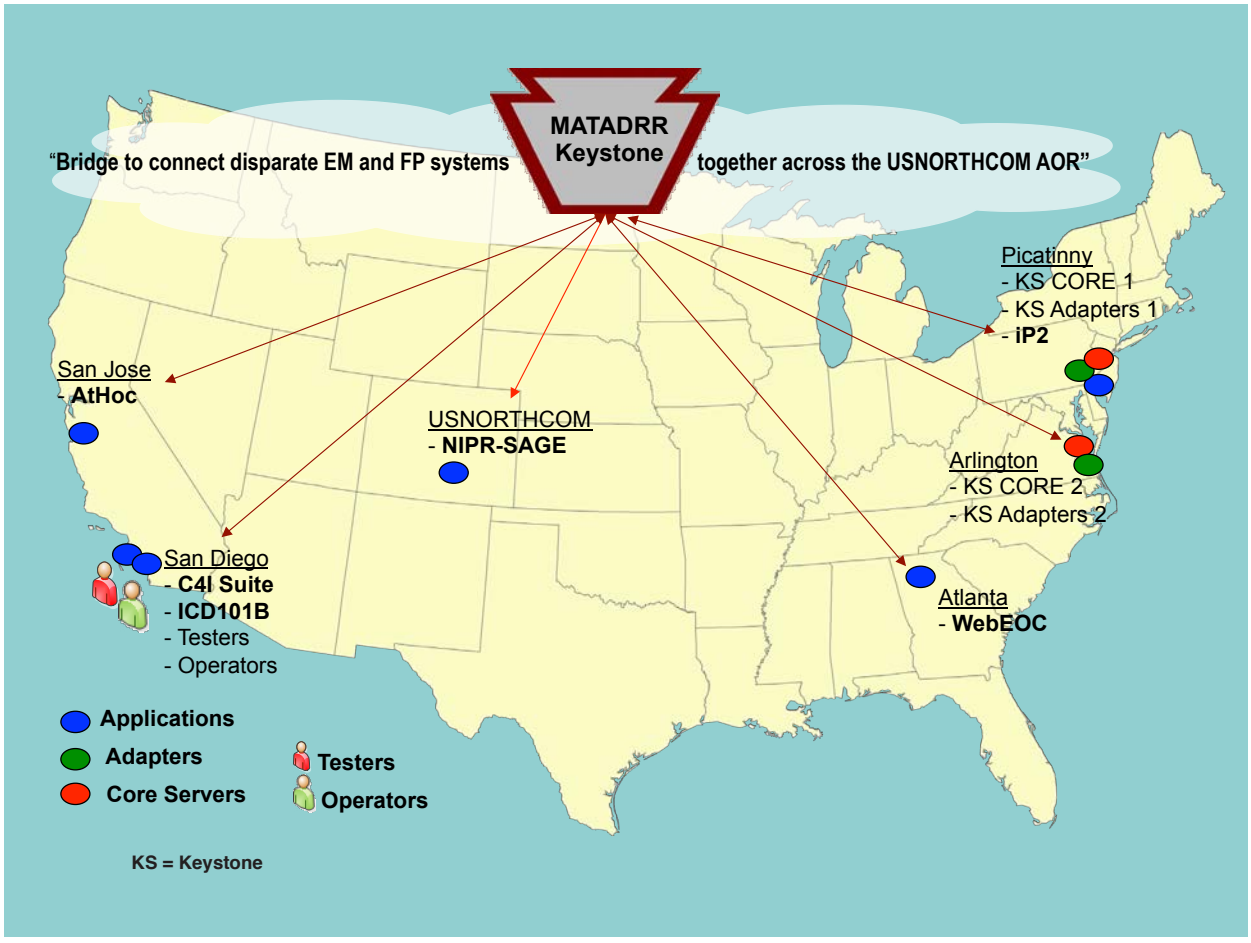



*Figure 7. MATADRR FXD Distributed Network*

### *Joint Interoperability Test Command (JITC) Assessment*

A JITC representative joined the Testers near the end of the IVT and began collecting log data from all communications between Keystone Cores, Keystone Adapters, and the native EM systems. After the IVT and FXD, this data will be further analyzed in terms of interoperability and standards, and the results will be provided in a JITC Assessment Report. This Product Reference Guide was submitted prior to the results of the JITC Assessment Report being available in May 2014. Information is available by request. Please contact Ms. Peggy West, peggy.west@us.army.mil.

## Final Transition Demonstration (FXD) (San Diego)

After a month-long IVT that finished with an End-to-End (E2E) System Test and a Joint Interoperability Test Command (JITC) Assessment, the FXD took place from 17-20 March 2014. It was the culmination of a USNORTHCOM operationally sponsored project addressing identified DoD-wide information sharing gaps. Over the course of three days, operator, technical, and observer feedback was collected and a final Operational Utility Assessment (OUA) was performed.

***Figure 8. FXD Kickoff Instructions for Operators, Subject Matter Experts, and Assessors***

Uniformed and civilian operators, subject matter experts, senior observers, operational assessment analysts, and key stakeholders observed the Operational Utility and User Feedback event conducted during the FXD and assessed first-hand the value added in the automated near real-time sharing of information supporting Force Protection and Emergency Management mission essential functions.

A series of scenarios and vignettes were used to exercise the EM/FP systems through the MATADRR Keystone middleware. Scenarios included terrorist events (a gate runner combined with a chlorine tanker truck explosion and a Mumbai-style attack with multiple shooters) and natural disasters (a hurricane along the eastern seaboard and an earthquake). Linked by Keystone, the previously disparate systems demonstrated the ability to share information and data, and display it on their respective situational awareness displays. Figure 9 demonstrates the power of Keystone: all five systems in the FXD display a plume that was generated after a chlorine tanker explosion and a subsequent chemical plume drifting southwest from the origin of the explosion. Without Keystone to initiate the exchange of data, these five systems cannot and do not inherently share information.

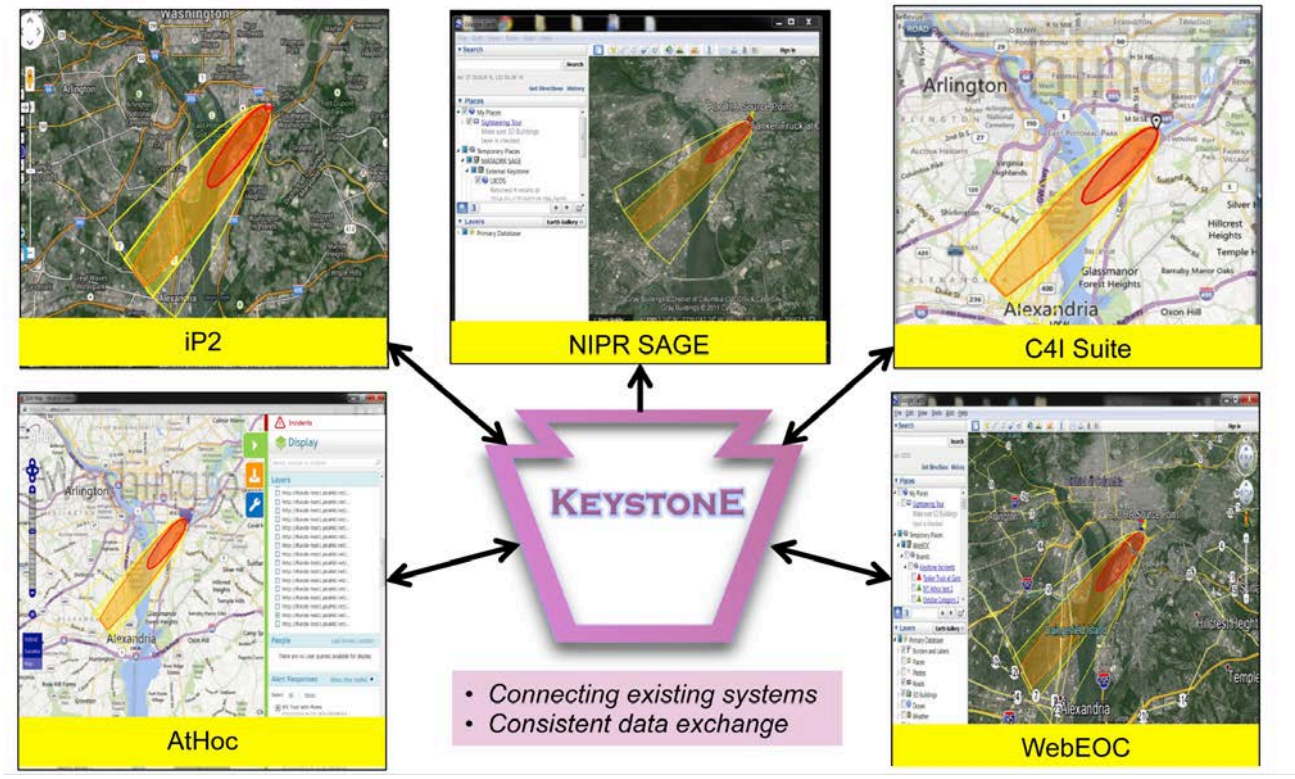



***Figure 9. Keystone—Information Sharing Across Systems***

### *FXD Outcomes*

- Initial findings indicate that planned Keystone functionality in an operationally relevant environment performed as expected, and information was shared between disparate systems in near real time.
- Critical feedback, comments and recommendations were collected for prioritization and incorporation into the next version of Keystone.
- Several capabilities were captured for future enhancements.
- The FXD identified the need for more in-depth conversations with the services and key stakeholders regarding concepts of employment and tactics, techniques and procedures (TTPs).
- Initial findings indicate that all planned Keystone functionality performed as expected.
- Initial responses from operators/analysts and subject matter experts were positive.
- Overall, users were satisfied with the functionality Keystone provided.
- Increased information sharing brought into focus the need for established business rules.
- Development of business rules is critical to successful deployment of Keystone capability.
- Initial feedback suggests Keystone will improve situational awareness and decision making for emergency management and force protection communities.

### *Joint Test and Assessment Group (JTAG) Operational User Assessment (OUA)*

Prior to the release of the full OUA report in early May, the JTAG provided an FXD Quick Look Assessment Report in early April. Key points are as follows:

This Product Reference Guide was submitted prior to the release of the final JTAG Operational User Assessment Report. Information is available by request. Please contact Ms. Peggy West, peggy.west@us.army.mil.

***Figure 10. FXD Operational Utility Assessment Instructions***

There were approximately 50 visitors participating in a variety of ways to support the FXD. A key transition partner stated, “I’m amazed at how far along the MATADRR team got within the 18 months timeframe. What a great capability.” – Ms. Karen House. Key stakeholders and participants are pictured below (Figure 11) at Space and Naval Warfare Systems Center, Pacific (SPAWARSYSCENPAC) in San Diego, CA, including representatives from:

- USNORTHCOM
- Air Forces Northern (AFNORTH)
- Army Northern (ARNORTH)
- Physical Security Enterprise and Analysis Group (PSEAG)
- Commander Navy Installations Command (CNIC)
- United States Fleet Forces Command (USFF)
- Commander Navy Region Southwest (CNRSW)
- National Guard Bureau (NGB)
- Armaments Research Development and Engineering Center (ARDEC)
- Engineer Research and Development Center (ERDC)
- San Diego County Emergency Operations Center (EOC)
- Carlsbad Fire
- Encinitas EOC
- Joint Project Manager Guardian (MATADRR Technology Transition Agreement partner)


***Figure 11. FXD Team and Stakeholders, SPAWARSYSCENPAC, San Diego, 20 March 2014***

# 5 Other Transition Key Stakeholders

There are many organizations and efforts that have influenced the development of the MATADRR products. In addition to the requirements generated from the Fort Hood and Navy Yard shootings, we have additional stakeholders that have helped shape products, adjust business rules and provide considerations for new software adapters.

## DSEA

The Defense Security Enterprise Architecture (DSEA) is a sister project of MATADRR, sponsored by the OSD's Physical Security Enterprise and Analysis Group (PSEAG), and represents a superset – information sharing – architecture effort. Its mission is to protect forces, mitigate threats, close protection gaps, and provide increased situational awareness by linking the disparate physical, personnel, information, industrial and operations security domain capabilities across the DoD while leveraging other government agencies' information. Keystone is intended to be a part of the DSEA solution set and is planned to be used in future DSEA Technical Demonstrations.

## DHS S&T UICDS

The Keystone software originated with the Department of Homeland Security (DHS) Directorate of Science and Technology (S&T). They developed and fielded the Unified Incident Command and Decision Support (UICDS), a similar national information sharing middleware, to share Common Operational Data (COD) and deliver information sharing in operational support of the National Incident Management System. The Keystone software will be provided to them at the end of the program.

## USPACOM/PDC

USPACOM has both a homeland defense and deployed mission requirement. USPACOM has provided key information about how the response to and coordination for a significant event would occur inside their area of responsibility. USPACOM represents a key stakeholder on how to develop an integrated operational picture across the local, state and military environment where they operate. Considerations such as the inclusion of electronic 911 services were provided to the MATADRR leadership from USPACOM.

Pacific Disaster Center (PDC) is an applied science, information and technology center, working to reduce disaster risks and impacts on life, property, and the economies worldwide. PDC's products and services are used to support sound decision making in disaster response and civil-military humanitarian assistance operations, as well as in disaster risk reduction, mitigation and planning. PDC resources are used locally and globally by disaster and crisis management professionals, planners and executive decision makers, national governments, regional organizations, and International and Non-Governmental Organizations (I/NGO). In particular, PDC is a key provider of data and information services to USPACOM for natural and manmade disasters. PDC leadership met with the MATADRR team to discuss potential information exchange with their DisasterAWARE product.

## TaCBRD/USEUCOM

The Transatlantic Collaborative Biological Resiliency Demonstration (TaCBRD) is a collaborative program between the U.S. Department of Defense (DoD), the U.S. Department of State (DOS), and the U.S. Department of Homeland Security (DHS). The Partner Nation for this program is the Republic of Poland. TaCBRD's objectives, with USEUCOM representing the operational manager, are to develop and demonstrate a capability for resilience in countering a wide-area biological incident that impacts U.S. and Partner Nation civilian and military personnel and key infrastructure.

Further, the USEUCOM Commander has authorized a technical demonstration and series of exercises using Keystone to better connect Host Nation support to the military installations, as well as, better connect forward staging bases back to higher command.

# 6 Other Related Events and Activities

## Assessment IPT

An Assessment IPT was established in July 2013, following Technology Demonstration #1, to provide a cross-coordinated focus working group to shape the assessments proposed as part of the Independent Verification Test (IVT) with a Joint Interoperability Test Command (JITC) assessment, and the Final Transition Demonstration (FXD) with an Operational Utility Assessment (OUA). The final task for the members of the Assessment IPT will be to review and provide feedback on the IVT and FXD assessment reports that will be available about one month post FXD, and recommend if any future assessments will be necessary for the project.

## CONOPS Working Group

The Concept of Operations Working Group (WG) was established in late 2012 to bring together Emergency Management and Force Protection analysts and operational planners from across the Services and the DoD agencies:

- to help develop and describe how MATADRR would enable greater shared awareness in Force Protection and Emergency Management operations horizontally across DoD and Civilian sectors
- to address problems/gaps of timely cross-service sharing of information
- to help define how MATADRR would enable rapid access to regional/local data and information.

The CONOP workshop addressed command and control arrangements needed to implement MATADRR. The CONOP described the processes and gaps associated with producing and rapidly disseminating actionable information in a Joint environment.

The initial WG was composed of the attendees listed in the following table.

| NAME | ORGANIZATION | EMAIL |
|---|---|---|
| **EXTERNAL ATTENDEES** | | |
| Bill Anderson | Software Engineering Institute-Carnegie Mellon University | wba@sei.cmu.edu |
| Gene Cahill | Software Engineering Institute-Carnegie Mellon University | gmcahill@sei.cmu.edu |
| Bob Chapman | Camber Corporation | rchapman@camber.com |
| Glenn Jagger | MARFORNORTH | glenn.jagger2@usmc.mil |
| Frank Comer | National Geospatial-Intelligence Agency (NGA) | comerf@gmail.com |
| Andre Leassear | IP2 Developer (EM2P) | leonard.a.leassear.ctr@mail.mil |
| Heather Keathly | Army G2- ATMIS | heather.a.keathly.civ@mail.mil |
| John Bender | AFNORTH A7X Emergency Management Specialist | john.bender@tyndall.af.mil |
| Leonard Jordan | AFNORTH A7X Emergency Management Specialist | leonard.jordan@tyndall.af.mil |
| LtCol Jeff Hollman | USAF AFSFC/SFOZ | jeffry.hollman@us.af.mil |
| John Seeley | CNIC N37 | john.r.seeley1.ctr@navy.mil |
| CDR Chris Gallagher | CNIC N37 | chris.gallagher@navy.mil |
| Bob Whitkop | CNIC 6.1 | robert.whitkop.ctr@navy.mil |
| Ray Roberts | Installation Base Defense | rroberts@cortek.com |

| NAME | ORGANIZATION | EMAIL |
|---|---|---|
| Tim Gourdine | Installation Base Defense | timothy.gourdine.ctr@us.army.mil<br>gourdine.timothy@bah.com |
| MSgt Salvione | HQ AFSPC Cmd Cnt Superintendent, AFSPC/A3OC | kathleen.salvione@us.af.mil |
| Richard Eicher | CFM for 1C3s (Pentagon) | richard.eicher@pentagon.af.mil |
| MAJ Ryan Leuders | USARNORTH | ryan.leuders@us.army.mil |
| LTC Andrew Gilman | USARMY RDECOM Science Advisor to N-NC | andrew.l.gilman@us.army.mil |
| George Randall | Applied Research Associates | george.randall.ctr@northcom.mil<br>grandall@ara.com |
| | | |
| **MATADRR TEAM ATTENDEES** | | |
| Jorge Zambrana | USNORTHCOM S&T Operations Manager/ Program lead | jorge.zambrana@northcom.mil |
| Tom Baron | USNORTHCOM J34 | thomas.baron@northcom.mil |
| Dave Hotop | USNORTHCON CTR. Deputy OM | NIPR: david.hotop.ctr@northcom.mil<br>Corporate: dhotop@camber.com |
| Shawn Schulze | USNORTHCOM CTR | NIPR: shawn.schulze.ctr@northcom.mil<br>SIPR: shawn.schulze@northcom.smil.mil<br>Corporate: sschulze@camber.com |
| Mike Spencer | USNORTHCOM CTR | mspencer@camber.com |
| Don Fulloon | ARDEC – Technical Manager | donald.w.fulloon.civ@mail.mil |
| Bob Boden | ARDEC – Senior Developer | robert.boden5.ctr@mail.mil |
| Doug Hardy | SPAWAR Pacific – Transition Manager | douglas.hardy@navy.mil |
| Chris Russell | SPAWAR Pacific – Deputy Transition Manager | chris.russell1@us.army.mil |

# 7 Program Reference Materials

The following products make up the essential documentation detailing the development and launch of Keystone and its accompanying policies. Information is available as indicated below on the http://www.matadrr.org website or by request; please contact Ms. Peggy West, peggy.west@us.army.mil.

## Key Presentations

The following presentations are available on the MATADRR web site: http://www.matadrr.org

**Information Brief:** Provides an overview of MATADRR that defines its operational goals, requirements, and road map.

**MATADRR Transition Brief:** Describes the process for transitioning the technology, knowledge products, and policy recommendations that comprise the MATADRR program.

**MATADRR Demonstration Videos R13.05 and R14.01:**

- Describes how MATADRR shares information across services
- Demonstrates its scalability of information, by transferring information across multiple Keystone Cores
- Provides examples of MATADRR business rules

**MATADRR FXD VIP Brief:** Provides an FXD overview of MATADRR for key stakeholders.

## Doctrine, Organization, Training, Material, Leadership, Personnel, Facilities, and Policy (DOTMLPF-P) Information Sharing Policy Recommendations

The MATADRR Project will provide DOTMLPF-P change recommendations by the project closeout. The Joint Test Assessment Group (JTAG-SPAWAR Atlantic) will formally submit this information via the Operational User Assessment (OUA) Report from the Final Transition Demonstration (FXD). The following lists a few of the preliminary findings on unclassified information sharing.

### *Horizontal Information Sharing*

- MATADRR allows bi-directional cross-service information sharing at the installation level utilizing EM /FP systems such as iP2 and C4IS.
- MATADRR allows one-way cross-service information sharing at the installation level utilizing NIPR-SAGE.
- The current version of AtHoc is a mass warning notification system, not an EM system. AtHoc is demonstrating a true EM system later this year.
- Cross-service information sharing above installation level is currently done ad-hoc using e-mail (and occasionally DMS). Cross-service information sharing above installation level could be accomplished by using NIPR-SAGE, but this is a single direction—as information is simply posted to a layer within NIPR-SAGE.

### *Vertical Information Sharing*

- The Department of the Navy has implemented C4IS at all levels of command for bi-directional information sharing.
- Vertical information sharing in the Army is hindered by higher echelons using different EM systems than are used at installations.
- Army installations can only share information with their higher headquarters via e-mail (bi-directional) and NIPR-SAGE (one-way).

## CONOPS/CONEMP

The MATADRR Joint Concept of Operations (CONOPS) prescribes an automated method for Force Protection reporting and Emergency Management information sharing through a back end application interface to improve timeliness and shared awareness. This CONOPS (in draft):

- Provides information on the FP/EM automated processes
- Aligns MATADRR development with the Defense Security Enterprise Architecture (DSEA), National Response Framework

(NRF), National Incident Management Systems (NIMS) and the DoD Mission Assurance Strategy

- Addresses business rules for data exchange among automated FP/EM tools and systems, resulting in cross-component automated information sharing mission capability to address shared situational awareness of all hazard threats.

The MATADRR Concept of Employment (CONEMP) explains how the MATADRR technical solution integrates within USNORTHCOM assigned missions. The CONEMP describes the processes for sharing information in a joint environment. It addresses the automated and timely cross service / agency sharing of unclassified information. This document describes how MATADRR and its software component, Keystone, translates unclassified messages, software application data and Geographic Information Systems (GIS) data among disparate systems for Force Protection and Emergency Management.

## IVT/FXD Keystone System/Software Requirements Document

The IVT/FXD Keystone System/Software Requirements Document describes the requirements and specifications used in the software development of the Keystone product targeted for use in the IVT and FXD (Keystone R14.01). Information is available by request. Please contact Ms. Peggy West, peggy.west@us.army.mil.

## Test and Assessment Reports

This Product Reference Guide was submitted prior to the results of many of the Test and Assessment Reports becoming available in May 2014. Information is available by request. Please contact Ms. Peggy West, peggy.west@us.army.mil.

The following is the summary list of MATADRR Test and Assessment Documents available:

- Joint Test Assessment Group (JTAG) MATADRR Technical Demonstration Letter of Observation – June 2013
- JTAG Final Transition Demonstration (FXD) Quick Look Report – April 2014
- SSC PAC Independent Verification Test (IVT) Report – May 2014
- JTAG FXD Operational Utility Assessment (OUA) Report – May 2014
- Joint Interoperability Test Command (JITC) IVT/FXD Assessment Report – May 2014

# Appendix A: Acronyms

| ACRONYM | DEFINITION |
|---|---|
| AAFES | Army and Air Force Exchange Service |
| ADD | Architecture Description Document |
| AFNORTH | Air Forces Northern |
| AOR | Area of Responsibility |
| API | Application Programming Interface |
| ARDEC | Armament Research, Development and Engineering Center |
| ARNORTH PMO | Army North Provost Marshall's Office |
| ASD-NM | Assistant Secretary of Defense for Nuclear Matters |
| ATO | Authorization to Operate |
| | |
| C4IS | Command, Control, Communication, Computers, and Intelligence Suite |
| CAD | Computer-Aided Dispatch |
| CAP | Common Alerting Protocol |
| CNRSW | Commander Navy Region Southwest |
| CoN | Certificate of Networthiness |
| COD | Common Operational Data |
| CONOPS/CONEMP | Concept of Operations/Concept of Employment |
| COP | Common Operating Picture |
| | |
| DHS | Department of Homeland Security |
| DIACAP | Department of Defense Information Assurance Certification and Accreditation Process |
| DISA | Defense Information Systems Agency |
| DLA | Defense Logistics Agency |
| DoD | Department of Defense |
| DOS | Department of State |
| DOTMLPF-P | Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities and Policy |
| DSEA | Defense Security Enterprise Architecture |
| DTA | Data Transition Agreements |
| DTRA | Defense Threat Reduction Agency |
| DTIC | Defense Technical Information Center |
| | |
| E2E | End-to-End |
| EDXL | Emergency Data Exchange Language |
| EM2P | Emergency Management Modernization Program |
| EM/FP | Emergency Management/Force Protection |
| EOC | Emergency Operations Center |
| ERDC | Engineer Research and Development Center |
| ESB | Enterprise Service Bus |
| | |

| ACRONYM | DEFINITION |
|---|---|
| FEMA | Federal Emergency Management Agency |
| FXD | Final Transition Demonstration |
| | |
| GIS | Geographic Information Systems |
| GOTS | Government Off-the-Shelf |
| | |
| HTTPS | Hypertext Transfer Protocol Secure |
| | |
| IAP | Incident Action Plan |
| IATO | Interim Authority to Operate |
| ICD | Interface Control Documents |
| ICP | Incident Command Post |
| ICS | Incident Command System |
| IMCOM | Installation Management Command |
| I/NGO | International and Non-Governmental Organizations |
| iP2 | Installation Protection Integration Platform |
| IPAWS | Integrated Public Alert and Warning System |
| IPT | Integrated Product Team |
| IT | Information Technology |
| IV&V | Independent Verification and Validation |
| IWS | Integrated Web Services |
| | |
| JAR | Java Archive |
| JAXB | Java API for XML Binding |
| JEM | Joint Effects Model |
| JITC | Joint Interoperability Test Command |
| JMS | Java Messaging Services (Java API) |
| JPM | Joint Project Manager |
| JPMG | Joint Project Manager Guardian |
| JTAG | Joint Test Assessment Group |
| JWARN | Joint Warning and Reporting Network |
| | |
| KML | Keyhole Markup Language |
| | |
| MAC II | Mission Assurance Category Level II |
| MATADRR | Mission Assurance, Threat Alert, Disaster Resiliency and Response |
| | |
| NETCOM | Network Enterprise Technology Command |
| NCR | National Capital Region |
| NGB | National Guard Bureau |
| NIEM | National Information Exchange Model |
| NIMS | National Incident Management System |
| NIPR SAGE | Non-Secure Internet Protocol Router Situational Awareness Geospatial Enterprise |

| ACRONYM | DEFINITION |
|---|---|
| OASIS | Organization for the Advancement of Structured Information Standards |
| OUA | Operational Utility Assessment |
| | |
| PDC | Pacific Disaster Center |
| POA&M | Plan of Action & Milestones |
| PRG | Product Reference Guide |
| PSEAG | Physical Security Enterprise and Analysis Group |
| PUB/SUB | Publish and Subscribe |
| | |
| REST | Representational State Transfer |
| | |
| S&T | Science and Technology |
| SA | Situational Awareness |
| SDD | System-Subsystem Design Document |
| SDK | Software Development Kit |
| SEIWG | Security Equipment Integration Working Group |
| SIP | System Identification Profile |
| SOA | Service Oriented Architecture |
| SOAP | Simple Object Access Protocol (XML protocol) |
| SPAWAR | Space and Naval Warfare |
| SPAWARSYSCENPAC | SPAWAR Systems Center Pacific |
| SSL | Secure Sockets Layer |
| | |
| TaCBRD | Transatlantic Collaborative Biological Resiliency Demonstration |
| TCP | Transmission Control Protocol |
| TNT | Technology and Transition |
| TTA | Technology Transition Agreement |
| TTP | Tactics, Techniques and Procedures |
| | |
| UICDS | Unified Incident Command and Decision Support |
| USEUCOM | U.S. European Command |
| USFF | United States Fleet Forces Command |
| USMTF | United States Message Text Format |
| USNORTHCOM | U.S. Northern Command |
| USPACOM | U.S. Pacific Command |
| | |
| WDSL | Wireless Digital Subscriber Line |
| WebEOC | Web Based Emergency Operations Center |
| WG | Working Group |
| | |
| XML | Extensible Markup Language |

## Appendix B: Key Stakeholder and Partner POC Information

| Organization | POC Name | Title | Phone | e-mail |
|---|---|---|---|---|
| ASD-NM PSEAG Office of the Secretary of Defense (OSD-NM-CBD) | Tom Whittle | Civ | 215.847.3104 | tom.whittle@navy.mil |
| OSD AT&L PSEAG | Steve Ellis | Civ | | leslie.ellis.ctr@osd.mil |
| USNORTHCOM S&T | Ed Doray | Civ | 719.554.1353 | edmund.doray@northcom.mil |
| USNORTHCOM S&T | Jorge Zambrana | Civ | 719.556.7457 | jorge.zambrana@northcom.mil |
| USNORTHCOM J34 | Tom Baron | Civ | 719.556.8700 | thomas.baron@northcom.mil |
| USNORTHCOM, J34 | LTC Michelle Thompson | Military | 719-554-7130 | michelle.thompson@northcom.mil |
| USNORTHCOM S&T Support | Dave Hotop | Civ | 719.359.7910 | dhotop@camber.com |
| USNORTHCOM S&T Support | Shawn Schulze | Civ | 719.685.7525 | sschulze@camber.com |
| USNORTHCOM S&T Support | Mike Spencer | Civ | 719.426.7759 | mspencer@camber.com |
| USNORTHCOM DISA Liaison | Marcial Dumlao | Civ | | marcial.b.dumlao.civ@mail.mil |
| USNORTHCOM S&T | Chris Thomas | Civ | 719.554.3378 | chris.thomas@northcom.mil |
| USNORTHCOM NIPR SAGE POC EM2P | David McKinley | Civ | 719.554.4950 | david.mckinley@northcom.mil |
| USNORTHCOM JPEO-CBD LNO | Paul Mugford | Civ | 719.554.7842 | paul.mugford.ctr@northcom.mil |
| ARDEC | Mike Cazzola | Civ | 973.724.1971 | michael.w.cazzola.civ@mail.mil |
| ARDEC | Bob Giarattano | Civ | 973.303.3814 | robert.m.giarratano.civ@mail.mil |
| ARDEC | Bryan Petzinger | Civ | 973-724-7018 | bryan.petzinger.ctr@mail.mil |
| ARDEC | George Foley | Civ | 732-319-3102 | george.b.foley.ctr@mail.mil |
| ARDEC | Charles Chapman | Civ | 973-724-1515 | charles.r.chapman2.civ@mail.mil |
| ARDEC | Italo Grasso | Civ | 973-724-8052 | italo.g.grasso.civ@mail.mil |
| ARDEC | Aisha Mims | Civ | 973-724-4004 | aisha.t.mims.civ@mail.mil |
| SPAWAR Systems Center Pacific | James Boerke | Civ | 619.553.4910 | james.boerke@navy.mil |
| SPAWAR Systems Center Pacific | Doug Hardy | Civ | 619.553.5410 | douglas.hardy@navy.mil |
| SPAWAR Systems Center Pacific | Peggy West | Civ | 619.553.6899 | peggy.west@us.army.mil |
| SPAWAR Systems Center Pacific | Ritesh Patel | Civ | 619.553.4509 | ritesh.patel@navy.mil |
| SPAWAR Systems Center Pacific | Cheryl Putnam | Civ | 619.553.4002 | cheryl.putnam@navy.mil |
| SPAWAR Systems Center Pacific | Paul Iordanides | Civ | 619.553.3616 | paul.iordanides@navy.mil |

| Organization | POC Name | Title | Phone | e-mail |
|---|---|---|---|---|
| SPAWAR Systems Center Pacific Support | Carol Nelepovitz | Civ | 858.401.2653 | carol.c.nelepovitz@saic.com |
| SPAWAR Systems Center Pacific Support | Chris Russell | Civ | 703.915.2338 | chris.russell1@us.army.mil |
| SPAWAR Systems Center Pacific Support | Ed Quismorio | Civ | 858.444.8216 | edgar.h.quismorio@ausgar.com |
| SPAWAR Systems Center Atlantic | Richard Baker | Civ | 843.218.4437 | richard.l.baker@navy.mil |
| SPAWAR Systems Center Atlantic | Paul Walter | Civ | 843.218.4795 | paul.walter@navy.mil |
| SPAWAR Systems Center Atlantic | Bill Knippenberg | Civ | 843.218.7934 | william.knippenberg@navy.mil |
| SPAWAR Systems Center Atlantic | Brian Spell | Civ | 843.218.5265 | brian.r.spell@navy.mil |
| SPAWAR Systems Center Atlantic | Jonathan McConnell | Civ | 843.218.2045 | johnathan.mcconnell@navy.mil |
| SPAWAR Systems Center Atlantic, Joint Test Assessment Group | Donald Lowe | Civ | 843.518.1655 | donald.lowe.4@us.af.mil |
| SPAWAR Systems Center Atlantic, JIGSAW-USMC Security Branch | Norbert Stiepel | Civ | 843.218.3704 | norbert.stiepel@navy.mil |
| U.S. Pacific Command - J348 - Branch Chief | Kevin P. Walker | Civ | 808.477.9405 | kevin.p.walker@pacom.mil |
| Pacific Disaster Center HS/HD Advisor | Steve Recca | Civ | 719.640.4346 (c) | |
| Pacific Disaster Center GIS- DC Metro | Malinda Braland | Civ | 703.614.1030 | mbraland@pdc.org |
| Pacific Disaster Center, Science Advisor | Dr. Heather Bell | Civ | 808.891.7942 | hbell@pdc.org |
| HQ US Central Command Emergency Manager (CCHC-EM) | Thomas Nunn | Civ | O: 813.827.2704<br>BB: 813.407.2383 | nunntd@centcom.smil.mil thomas.nunn@centcom.mil thomas.nunn.2@macdill.af.mil |
| US EUROPEAN COMMAND (EUCOM) ECJ8-Q S&T Division | Joe Fagan | Civ | (49) (0) 711.680.8955 | joe.fagan@eucom.mil |
| US Strategic Command (STRATCOM) | Rich Delong | Civ | 402.294.3183 | delongr@stratcom.mil |
| Research, Development and Engineering Command (RDECOM) | Eddie Ansell | Civ | 410.278.8596 | eddie.g.ansell.civ@mail.mil |
| US Southern Command (SOUTHCOM) SCJ7 | Donald Jones | Civ | | donald.jones@hq.southcom.mil |
| Defense Security Enterprise Architecture (DSEA) | Monte Murphy | Civ | 703.412.9425 | mmurphy@ara.com |
| Defense Security Enterprise Architecture (DSEA) | George Randall | Civ | 719.622.6133 | grandall@ara.com |
| Joint Project Manager Information Systems (JPM-IS) | Les Anderson | Civ | 619.553.4045 | les.anderson@jpmis.mil |
| JPEO-CBD (IBD) | George “Ed” Lawson | Civ | 410.436.4832 | george.e.lawson.civ@mail.mil |
| National Guard Bureau (NGB) AT / FP Officer | Captain Christina Hardy | Military | | christina.hardy@us.army.mil |

| Organization | POC Name | Title | Phone | e-mail |
|---|---|---|---|---|
| National Guard Civil Support (NGCS) Requirements Planning (NGB/A3D) Senior Advisor | Ken “Batman” Franklin | Civ | 240.612.8235 | kenneth.franklin.ctr@ang.af.mil |
| NGB GeoGuard - NGB/J336 | Dr. Brian Cullis | Civ | 720.872.4427 | brian.cullis@critigen.com |
| NGB GeoGuard - NGB/J336 | Charles Snyder | Civ | | charles.snyder3@us.army.mil |
| NGB J8 | Juan L. Orama | Civ | 703.607.1256 | juan.l.orama.ctr@mail.mil |
| NGB J8 rep | Jaun Orama | Civ | 703.607.1256 | juan.orama@us.army.mil |
| NGB | Major Bowlsbey | Military | | bryan.w.bowlsbey.mil@mail.mil |
| NGB, Chief NG-J6/CIO-C4 Division | LTC Tom Pettit | Military | 703.601.2651 | timothy.o.pettit.mil@mail.mil |
| NGB Integrator at N-NC | Major Rich Szabo | Military | 719.554.1595 | rich.szabo@northcom.mil |
| California Air National Guard | SSG Justin McCauley | Military | 916.854.3440 | justin.mccauley@us.army.mil |
| ARNORTH PMO | Robert Ake | COL | 210.221.2330 | robert.ake@us.army.mil |
| ARNORTH PMO | Craig Hinman | Civ | 210.221.1999 | craig.n.hinman.civ@mail.mil |
| ARNORTH Science Advisor | LTC Ryan Lueders | Military | 210-221-2525 | ryan.p.lueders.mil@mail.mil |
| IMCOM DEPUTY Prot Off/ FP /EM | Floyd Williams | Civ | 210.466.0115 | floyd.williams@us.army.mil |
| Installation Management Comd Pgm Mgt Office (IMCOM PMO) | COL Bradley Graul | Military | 210.466.0115 | bradley.graul@us.army.mil |
| Dir, Security Forces, District of Washington | Mark Allen | Civ | 240.612.6420 | mark.allen@afncr.af.mil |
| Lackland AFB 802nd CE SQ | Willie J. Gibbs III | Civ | 210.671.2260 | willie.gibbs.1@us.af.mil |
| USAF SAF AQR, S&T Office | John Smith | Civ | | john.r.smith@pentagon.af.mil |
| USAF Emergency Manager | Mike Connors | Civ | 850.283.6165 | mike.connors@tyndall.af.mil |
| USAF Emergency Manager | John Jennings | Civ | 850.283.6214 | john.jennings@tyndall.af.mil |
| CONR-1AF (AFNORTH) / A8 | Maj Ivan Wood | Military | 850.283.8040 | ivan.wood@tyndall.af.mil |
| Offutt AFB Installation Emergency Manager | Rhonda Woolridge | Civ | 402.294.3642 | rhonda.woolridge@offutt.af.mil |
| HQ AFSPC Command Center | MSgt Kathleen Salvione | Military | | kathleen.salvione@us.af.mil |
| HQ USAF | Michael Messersmith | Civ | 210.784.7547 | michael.messersmith.2@us.af.mil |
| USAF A7SP | Leonard Jordan | Civ | | leonard.jordan@tyndall.af.mil |
| AFNORTH -AFCEC-EAST/CXR- Emergency Mgmt | Michael Surette | Civ | 850.283.6256 | michael.surette@tyndall.af.mil |
| AFNORTH/A7X | John Bender | Civ | 850.283.0173 | john.bender@tyndall.af.mil |
| AFNORTH/A7X | SMSgt Michael Pope | Military | | michael.pope@us.af.mil |
| AF/A7CX | Bill W. Thomas | Civ | 703.695.1785 | billy.thomas@pentagon.af.mil |

| Organization | POC Name | Title | Phone | e-mail |
|---|---|---|---|---|
| USAF HQ AFSFC/SFXR | Chuck Deatelhauser | Civ | 210.925.5660 | charles.deatelhauser.1@us.af.mil |
| Emergency Services Branch (A7CXR) | David Abruzzi | Civ | 703.697.6560 | david.abruzzi@pentagon.af.mil |
| Air Force Security Forces Center POC | LTC Jeffry Hollman | Military | 210.925.5157 | jeffry.hollman@us.af.mil |
| Joint Base Charleston SC | J. Dwayne Gunther | Civ | 843.963.7267 | |
| Joint Base Charleston SC | Olin (Tom) E. Thomas | Civ | 843.730.3211 | olin.thomas@us.af.mil |
| Joint Base Charleston SC | Sarah Winberry | Civ | | sarah.winberry.3@us.af.mil |
| MARFORNORTH AT/FP/EM | Randy Gholson | Civ | 504.697.9647 | randy.gholson@usmc.mil |
| MARFORNORTH AT/FP/EM | Glenn Jagger | MFN CIP- Mng | 504.697.9646 | glenn.jagger2@usmc.mil |
| USMC, HQ, Integrated Installation Protection (IIP) | Mark Brown | Civ | 703.614.7928 | mark.a.brown4@usmc.mil |
| US Marine Corps rep to SEIWG | Rodney Rourk | Chair-man, SEIWG | 843.218.4375 | rodney.rourk@navy.mil |
| HQMC MAAT | Doug Phelps | Tm Lead | 571.242.5523 | |
| Fleet Forces Command AT/EM/FP | Willard Thompson | Civ | 757.836.7758 | willard.thompson@navy.mil |
| Commander, Navy Installations Command (CNIC) N37 EM HQ Program Dir | CDR Chris Gallagher | Military | 202.433.4735 | chris.gallagher@navy.mil |
| CNIC N37 Operations PM | Garth Kaliczak | Civ | 202.433.9383 | garth.kaliczak@navy.mil |
| CNIC N37 | Daniel Haacke | Civ | 202.433.9337 | daniel.haacke@navy.mil |
| CNIC N6.1 | Gill Ward | Civ | XXXXX | gill.ward@navy.mil |
| CNIC N6.1 | Bob Whitkop | Civ | 904.638.4366 | robert.whitkop.ctr@navy.mil |
| CNIC N6.1 | Joe McConnell | Civ | | joe.mcconnell@navy.mil |
| CNIC N37 | John Seeley | Civ | | john.r.seeley1.ctr@navy.mil |
| Department of Homeland Security (DHS) OHA | Michael Walters | Civ | | michael.walters@dhs.gov |
| National Reconnaissance Office (NRO) | Gene Hoffman | Civ | | gene.hoffman@nro.mil |
| National Geospatial-Intelligence Agency (NGA), Chief | Frank Comer | Civ | 571.557.7878 | frank.w.comer@nga.mil |
| National Geospatial-Intelligence Agency (NGA), Deputy Chief | Sal A. Falzone | Civ | 571.557.7877 | sal.a.falzone@nga.mil |
| National Security Agency (NSA) | Steffan Arndt | Civ | | sparndt@nsa.gov |
| Defense Threat Reduction Agency (DTRA) | Chuck Sorge | Civ | 703.767.2975 | charles.sorge@dtra.mil |

| Organization | POC Name | Title | Phone | e-mail |
|---|---|---|---|---|
| Defense Threat Reduction Agency (DTRA) | Alfredo Guerrero | Civ | | alfredo.guerrero@dtra.mil |
| Defense Contract Management Agency (DCMA) | Liam Whooley | Civ | | liam.whooley@dcma.mil |
| Defense Contract Management Agency (DCMA) | Margret Devlin | Civ | | margaret.devlin@dcma.mil |
| Defense Logistics Agency (DLA) | Bruce Thomas | Civ | 703.767.1279 | bruce.thomas@dla.mil |
| Defense Logistics Agency (DLA) | Lynette Gruse | Civ | 703.767.5426 | lynette.gruse@dla.mil |
| Defense Logistics Agency (DLA) | Eric Linneman | Civ | 703.767.5019 | eric.linneman@dla.mil |
| Defense Information Systems Agency (DISA) DISA-PS CBRNE PM DEPT ATO | Timothy Chrysler | Civ | | timothy.j.chrysler.civ@mail.mil |
| Defense Information Systems Agency (DISA) DISA- IA, GS-15, Deputy - CIO | Paul Demennato | Civ | 301.225.8276 | paul.c.demennato.civ@mail.mil |
| Pentagon Force Protection Agency (PFPA) | John O'Niel | | | john.oniel@pfpa.mil |
| PFPA AT/FP CBRN POC: | Dan Walsh | | 703.697.2446 | dan.walsh@pfpa.mil |
| Joint Project Office-Guardian (JPM-G) S&T | COL James K. Choung | Military | 410.417.3593 | james.k.choung.mil@mail.mil |
| Joint Project Office-Guardian (JPM-G) S&T | Karen House | Civ | 410.417.3308 | karen.m.house.civ@mail.mil |
| Joint Project Office-Guardian (EM2P) | Andre Leassear | Civ | | leonard.a.leassear.ctr@mail.mil |
| Joint Project Office-Guardian (EM2P) | Greg Mrozinski | Civ | | gregory.p.mrozinski.civ@mail.mil |
| SEIWG Chairman | Rodney Rourke | Civ | 843.218.4375 | rodney.rourk@navy.mil |
| Deputy Chief CEM - South Carolina Emergency Management Division | V. Taylor Jones | Civ | 864.844.3005 | tjones@andersoncountysc.org |
| Global Combating Weapons of Mass Destruction Awareness System (GCAS) | Brett Bonifay | Civ | 619-221-7275 | brett.bonifay@jpmis.mil |
| Global Combating Weapons of Mass Destruction Awareness System (GCAS) | MAJ David Smith | Military | 410.436.5515 | david.s.smith.mil@mail.mil |
| Global Combating Weapons of Mass Destruction Awareness System (GCAS) | Rick Avera | Civ | 540.284.0066 | rick.avera@navy.mil |
| Denver Urban Area Security Initiative (UASI) | Dan Alexander | Civ | 720.865.7600 | daniel.alexander@denvergov.org |
| Denver Urban Area Security Initiative (UASI) | Lin Bonesteel | Civ | 720.865.7659 | linda.bonesteel@denvergov.org |
| Integrated Base Defense (IBD) Support | Jeffry B. Jones | Civ | 702.735.6503 | jeff.jones@ndgi.com |
| IBD Lead Architecture & Analysis team | Karen Short | Civ | 256.658.0815 | karen.short@us.army.mil |
| IBD Senior Operations Analyst | Ray Roberts Jr | Civ | 540.891.8315 | rrobberts@cortek.com |

| Organization | POC Name | Title | Phone | e-mail |
|---|---|---|---|---|
| USDA APHIS | Lori Miller | Civ | | lori.miller@dhs.gov |
| Emergency Services Coordinator ACSO | SGT Richard C. Guinn | Military | 928.337.4321 | rguinn@co.apache.az.us |
| Def Installation Spatial Data Infastructure | David LaBranche | Civ | 571.372.6768 | david.labranche@osd.mil |
| JPMIS JWARN APM | Captain Mal Sandie | Military | 619.221.7712 | malachy.sandie@jpmis.mil |
| JPMIS JWARN DAPM | Mike Nichols | Civ | 619.221.7711 | mike.nichols@jpmis.mil |
| JPM IS Lead Architect | Andy Hill | Civ | 619.553.7661 | david.hill@jpmis.mil |
| JEM Acquisition Program Manager Joint Project Manager Information Systems (JPM IS) | Thomas Smith | Civ | 858.537.0497 | thomas.r.smith@jpmis.mil |
| JPM IS JEM Deployment | Mike Bingham | Civ | 858.537.0371 | mike.bingham@jpmis.mil |
| AAFES | Glen Smith | Civ | 214.312.6700 | |
| Pac NW Nat Lab | Michael Catalan | Civ | 509.528.1963 | michael.catalan@pnnl.gov |
| Software Engineering Institute | William Anderson | Civ | 412.268.5386 | wba@sei.cmu.edu |
| Software Engineering Institute | Jeff Boleng | Civ | 412.268.9595 | jlboleng@sei.cmu.edu |
| National Preparedness Support | Richard “Lex” Lexvold | Civ | 352.293.5897 | richard.lexvold@us.army.mil |
| Lawrence Livermore National Laboratory (LNNL) | Eric McKinzie | Civ | 925.422.9244 | mckinzie1@llnl.gov |
| LLNL Director Biodefense Knowledge Center | Dr. Tom Bates | Civ | 925.423.3055 | twbates@llnl.gov |
| LLNL PM | Anthony Totaro | Civ | 925.423.7747 | totaro1@llnl.gov |
| MIT Lincoln Laboratory (NICS) Next Generation Incident Command System | Gregory “Gregg” Hogan | Civ | 781.981.7425 | hogan@ll.mit.edu |
| MIT Lincoln Laboratory (NICS) Next Generation Incident Command System | Jose A. Vazquez | Civ | 202.254.6092 | jose.vazquez3@dhs.gov |
| MIT Lincoln Laboratory (NICS) Next Generation Incident Command System | Daniel M. Cotter | Civ | 202.254.6093 | david.cotter@hq.dhs.gov |
| DHS S&T | Rusty Dash | Civ | 202.447.3725 | russell.dash@hq.dhs.gov |
| DHS S&T | Andy Manley | Civ | 202.447.3376 | andrew.manley@hq.dhs.gov |
| HQ Department of the Army (HQDA) G2/34 | Heather Keathly | Civ | 703.695.2662 | heather.a.keathly.civ@mail.mil |
| HQDA G3, OPMG | Bill Black | COL | | william.r.black8.mil@mail.mil |
| HQDA G34, Protection | Daryle Hernandez | COL | | daryle.j.hernandez.mil@mail.mil |
| JFHQ-NCR | Erin Boscolo | Civ | 202.685.2577 | micheal.g.osterhoudt.civ@mail.mil |

| Organization | POC Name | Title | Phone | e-mail |
|---|---|---|---|---|
| Joint Staff, J36/CSOD | Lewis (Paul) Goodwin | LTC | 703.695.6571 | lewis.p.goodwin2.mil@mail.mil |
| Joint Staff, J36/CSOD | Dennis Sherrill | Civ | 703.695.6572 | dennis.l.sherrill.ctr@mail.mil |
| Joint Staff, J36/CSOD | Kimberly Baumgartner | Civ | 703.695.6573 | kimberly.a.baumgartner2.ctr@mail.mil |
| OSD EM | Ryan Broughton | Civ | | rbroughton@dpmsllc.com |
| OSD Mission Assurance | Neil Holloran | Civ | 540.653.0436 | neil.holloran@navy.mil |
| OSD AT&L (ARA) | Steve Ellis | Civ | 202.761.0671 | leslie.ellis.ctr@osd.mil |
| OSD AT&L (ARA) | Linda Parker | Civ | 703.412.9425 | linda.parker.ctr@osd.mil |
| OSD AT&L Program Analyst | Beki Gangi | Civ | 703.412.9425 | rgangi@ara.com |
| OSD-ATL - EMSG | Art Kaminski | Civ | | art.kaminski@osd.mil |
| U.S. Coast Guard-Incident Management Assistant Team (USCG-IMAT) | Spencer Templeton | Civ | 757.398.3901 | spencer.c.templeton@uscg.mil |
| USCG IMAT- Incident Mgt Asst Team | LCDR Kevin S. Hill | Military | 757.852.3411 | kevin.s.hill@uscg.mil |
| U.S. Coast Guard (CG-7612) | LCDR John Chang | Military | 202.372.1292 | john.v.chang@uscg.mil |
| AtHoc | Aviv Siegel | Civ | 650.291.9409 | asiegel@athoc.com |
| WebEOC | Tim Beltz | Civ | 970.219.5442 | tim.beltz@intermedix.com |
| Joint N-NC/Washington Operations | Jan P. Ithier | Civ | 703.695.4604 | jan.p.ithier.civ@mail.mil |
| Joint Staff, J34 | COL Mike Brobeck | Military | 703.614.0276 | micheal.w.brobeck.mil@mail.mil |
| Joint Staff, J34 | COL Bob Manion | Military | 703.614.0022 | robert.l.manion.mil@mail.mil |
| Joint Staff, J34 | COL Dan Evans | Military | 703.693.7522 | daniel.t.evans.mil@mail.mil |
| Joint Staff, J34 | MAJ Bobby Ford | Military | 703.614.0083 | robert.m.ford10.mil@mail.mil |
| Joint Staff, J34 | Rosemary Helton | Civ | 703.693.2111 | rosemary.k.helton.ctr@mail.mil |
| Joint Staff J34 AT/FP | Mike Osterhoudt | Civ | 703.693.7526 | |
| Joint Staff, J34 | Bryan Driskell | Civ | 703.695.0625 | bryan.b.driskell.civ@mail.mil |
| G34/EM2P Support (Davis-Paige) | Joe Ogelsby | Civ | 210.834.8104 | jogelesby@dpmsllc.com |
| G34/EM2P Support (Davis-Paige) | Ronald Griffis | Civ | 210.269.5671 | rgriffis@dpmsllc.com |
| Topographic Engineering Center Engineer Research and Development Center (ERDC) | Ritchie Rodebaugh | Civ | 703.428.6014 | ritchie.l.rodebaugh@usace.army.mil |
| Topographic Engineering Center Engineer Research and Development Center (ERDC) | Terrance Westerfield | Civ | 703.428.3597 | terrance.w.westerfield@usace.army.mil |
| Topographic Engineering Center, Engineer Research and Development Center (ERDC) | Eric Zimmerman | Civ | 703.428.6663 | eric.zimmerman@usace.army.mil |

| Organization | POC Name | Title | Phone | e-mail |
|---|---|---|---|---|
| Geospatial Research and Engineering Army Corps of Engineers Engineer Research and Development Center (ERDC) Topographic Engineering Center Alexandria, VA | Mike Tischler | Civ | 703.428.3699 | michael.a.tischler@usace.army.mil |
| CNRSW, N3 | Joseph Stuyvesant | Civ | | joseph.stuyvesant@navy.mil |
| CNRSW, N37 | Karen Blackwood | Civ | | karen.blackwood@navy.mil |
| CNRSW, N3 | Mark Frederickson | Civ | | mark.frederickson1@navy.mil |
| CNRSW, N3 | Kurt Stoney | Civ | | |
| San Diego County, EM EOC | Robbie Barreras | Civ | 858.715.2341 | robert.barreras@sdcounty.ca.gov |
| Encinitas City, EOC Coordinator | Tom Gallup | Civ | | tgallup@encinitasca.gov |
| Carlsbad Fire Department | David Harrison | Civ | 760.931.2137 | david.harrison@carlsbadca.gov |
| JITC/Combat Systems Branch | Janet Weese | Civ | 520.538.5358 | janet.r.weese.civ@mail.mil |



MATADRR

Mission Assurance, Threat Alert, Disaster Resiliency & Response

## *Postscript*

The MATADRR Transition Management Team would like to thank all of the contributors to this document. We hope that you found this document contained concise, valuable information about the Product and its Transition State as of June 2014. Further, we hope that it provided useful information about where to go and who to contact for additional product information. If you have feedback or ideas on how to improve this report, or have general comments or questions about the project, or specific questions about the products named herein, please email: peggy.west@us.army.mil or call: 619-553-6899. For an alternate point of contact, please email: douglas.hardy@navy.mil or call: 619-553-5410.

**Primary Authors:**
Douglas Hardy, MATADRR XM, SPAWAR Systems Center Pacific (SSC Pacific)
Christopher Russell, MATADRR DXM, SSC Pacific Contractor Support

**Chief Editors:**
Ashley Russell, MATADRR XM Team, SSC Pacific Contractor Support
Peggy West, MATADRR XM Team, SPAWAR Systems Center Pacific (SSC Pacific)

**Publishers:**
Art Armendariz, SPAWAR Systems Center Pacific (SSC Pacific)
Lee Hood, SPAWAR Systems Center Pacific (SSC Pacific)
Norman Tancioco, SPAWAR Systems Center Pacific (SSC Pacific)